Cahoy Supp. Dec. Ex. 90

Table of Contents

List of Attachments

Attachment #	Document Name	Document #
Attachment A	IS4000 Software Level of Concern	818421-40
Attachment B	Known Anomalies List for IS4000	827102-40 Rev C
Attachment C	IS4000 Cybersecurity Risk Analysis	818440-40
Attachment D	IS4000 Cybersecurity Requirements	818450-40
Attachment E	IS4000 Cybersecurity Risk Trace Matrix	818470-40
Attachment F	OnSite Product Overview	813331-33
Attachment G	Test Report for CyberSecurity & Penetration Testing	818460-40R

History of Responses

Deficiency Question	Description	FDA Follow up Questions - Date	ISI Response to FDA Feedback
1	Level of Concern	None	Responded to deficiency on 11/15/2013
2	Unresolved Anomalies	12/20/2013	Responded to deficiency on 11/15/2013, 01/10/2014, 02/19/2014
3	Cybersecurity	12/20/2013	Responded to deficiency on 11/15/2013, 1/10/2014, 02/19/2014
4	Run Time Error Detection	12/20/2013	Responded to deficiency on 11/15/2013and 1/10/2014

FDA Question 1 dated August 23, 2013

1. *Level of Concern*
   You concluded that the Level Of Concern (LOC) was MODERATE. The Agency considers this to be a MAJOR LOC device. Please correct your LOC.

ISI Response dated November 15, 2013

Intuitive Surgical has revised document 818421-40, *IS4000 Software Level of Concern*, to reflect the IS4000 as a MAJOR LOC device. The revised document is included as **Attachment A** in this response.

FDA Question 2 dated August 23, 2013

2. *Unresolved Anomalies (Bugs or Defects)*
   In Appendix 16, in the Section entitled Known Anomaly List, you provided a list of the remaining software anomalies. For several of these anomalies, you stated that that recovery may require power cycling i.e. turning the system off and then on. This is a concern. Please provide a more detailed description of these unresolved anomalies (UAs) and the possible adverse clinical effect(s), and then either mitigate these UAs or provide an acceptable explanation as to why these anomalies should remain extant.

ISI Response dated November 15, 2013

The IS4000 software implements a variety of run-time checks, which trigger the system fault reaction logic if they fail, and rapidly brings the system to a safe, motionless state. Each of these

run-time checks is classified as 'recoverable' or 'non-recoverable', which identifies whether the user can attempt to recover the fault without rebooting the system (recoverable) or if the user must reboot the system to continue (non-recoverable). The IS4000 system has been designed to allow the user to quickly restart (<120 sec.) the system in the middle of a procedure. The most common reason that a restart would be required is a non-recoverable fault detected by software, for example, due to a temporary power loss to the Vision Cart or Surgeon Console subsystems.

When a non-recoverable fault is encountered, the system is designed to provide the user clear notifications on all system graphical user interfaces, with instructions to restart the system to continue. The steps for a mid-procedure restart are described clearly in the system User Manual, and steps are also provided in the user manual on how to restart the system if it is unresponsive.

Unresolved anomalies are evaluated using a risk based approach, and the risk assessment for each anomaly is evaluated by a cross functional team to determine whether it is clinically acceptable. The worst case clinical condition allowed for a power cycle restart is a maximum 2 minute delay to the procedure. The number of anomalies that could result in a 'non-recoverable' fault is evaluated and reduced as much as reasonable during the software development process.

An updated Known Anomalies list will be provided with the formal response.

FDA Follow-up Question 2 dated December 20, 2013

2. *Unresolved Anomalies – power cycling:*

   The firm states that when the system enters certain states, the system must be rebooted to continue to operate. This explanation is acceptable for those states. However, the Unresolved Anomalies section addresses known bugs that remain extant in the to-be-released software version.

   The firm should not have any known bugs remaining in their software that need to have the system rebooted to continue. The bugs should be fixed!

ISI Follow-up Response dated January 10, 2014

Since the original submission, ISI has updated the system software (A7.0P2). All known anomalies in the previous version (A7.0P1) that required the system to be rebooted during surgery have been resolved. There are no known anomalies in the updated system software that require a system reboot during surgery.

During Power On, where a rigorous power-on self-check is conducted, a set of software anomalies exist where the user would need to power cycle the system to continue. A fundamental principle of the software design for the system is that it fail safe, and these anomalies that occur during the power-on self-check are consistent with that principle. These

anomalies have a low rate of occurrence, are resolved by rebooting the system, and do not represent a significant safety risk to the user and/or patient.

Does FDA agree that the presence of these anomalies does not represent a safety issue and is acceptable?

FDA Follow-up Question 2 dated January 23, 2014

FDA confirmed the information provided was acceptable.

ISI Follow-up Response dated February 19, 2014

An updated Known Anomalies list for A7.0P2 is provided in **Attachment B**.

FDA Question 3 dated August 23, 2013

3. *Cyber and Information security*
   You mention network communications as part of this system. There is not a separate Section addressing the CyberSecurity issues. Please review the Management of Cybersecurity Guidance issued 6/14/13 and provide information, as appropriate, on the Cybersecurity aspects of your device.

ISI Response dated November 15, 2013

In accordance with FDA's draft guidance "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" issued on June 14, 2013 Intuitive Surgical has prepared additional documentation to address cybersecurity concerns for the IS4000 system. Cybersecurity was considered in the design of the IS4000 system, but the guidance was released just a few days before the 510(k) was submitted. The following information is being provided in accordance with the guidance.

Cybersecurity Hazard Analysis

Document 818440-40, *IS4000 Cybersecurity Risk Analysis*, which has been included with this response (**Attachment C**), was created after analyzing security risks on all customer accessible ports and wireless interfaces. Mitigation of cybersecurity risks is accomplished by utilizing a layered approach which includes the following:

- Some communication ports are custom designs that would be difficult to reverse engineer,
- Authentication/encryption is used to control access to communicate with the port,

- Custom protocols are used for communicating between subsystems, and
- Safety system monitoring detects unrecognized commands.

Severity levels are defined in a manner consistent with ISI's risk analysis process where the possible harm if a customer accessible interface was compromised is identified, assuming no mitigations were in place. The *likelihood* of someone being able to compromise the interface is determined after considering the layered mitigations that are in place. Using the severity and likelihood levels, a risk index is computed. All risks have been mitigated to acceptable levels.

The specific list of cybersecurity controls for the IS4000 system is provided in document 818450-40, *IS4000 Cybersecurity Requirements*, which is included with this response (**Attachment D**). The list of controls includes all items identified in the Mitigations column of the risk analysis.

Cybersecurity Traceability Matrix

The linkage from mitigations in the cybersecurity risk analysis to the actual cybersecurity controls (requirements) is provided in document 818470-40, *IS4000 Cybersecurity Risk Trace Matrix*, which is included in this response (**Attachment E)**. The trace report documents the linkage from risks to requirements.

Cybersecurity Maintenance Plan

Updates to the *da Vinci* Surgical System software are released on a routine basis to incorporate new product features, known anomaly fixes, and security patches. Updates to operating systems and security libraries will be monitored and updated during these software releases. If a critical security patch is required, then a software update targeting that specific software component will be created, tested, and released. As security issues arise, Intuitive Surgical will evaluate them based on the cybersecurity risk analysis process, which will drive the appropriate response.

Cybersecurity Malware Certification

Intuitive Surgical implements safeguards against infection by malware throughout the entire software lifecycle, from initial design to releasing software to systems in the field. **Table** identifies the stages in Design, Manufacturing, and Field Service and identifies the mitigations that are in place to prevent malware.

Title

818440-40 Revision A, Cybersecurity Risk Analysis, IS4000

Table of Contents

Purpose

This document provides a system-level analysis of cybersecurity risks related to intentional or unintentional compromise of the IS4000 system. The analysis considers each customer-accessible and/or wireless interface in the system, and identifies risks due to unauthorized modification, misuse or denial of use of the system via each interface. The results of the analysis define the set of design mitigations and cybersecurity controls that ensure safe device operation in the face of cybersecurity risks.

Scope

This document applies to the IS4000 system only. The following participants were involved in the development of this analysis:

Revision	ECO	Scope of Analysis	Date of Analysis	Participant(s)/Department

A	C102219	Initial Release of Full Analysis	Nov 2013	Brian Miller / Engineering, John Seaman / Engineering, Zach Dickinson / Engineering, Tabish Mustufa / Engineering, Rex Wright / Risk Management, Brandon Hansen / Regulatory Affairs

References

854022 SOP, Risk Management Procedure
854136 DOP, Risk Analysis Guideline
818450-40 Cybersecurity Requirements, IS4000

Background

This risk analysis is constructed with guidance from SOP 854022 *Risk Management Procedure* and DOP 854136 *Risk Analysis Guideline*. Readers should consult these documents for further background and guidance.

The analysis was conducted according to DOP 854136 by identifying a Severity for each risk assuming no mitigations were in place. With mitigations documented, a Likelihood was defined. Using the Severity and Likelihood, a Risk Index was found.

There are four Severity rankings defined in DOP 854136. With respect to cybersecurity risks, these rankings are interpreted as follows:

- Catastrophic: Compromise of interface can lead to serious injury or death to the patient or user.
- Critical: Compromise of interface can lead to minor or significant surgical or clinical intervention, and results in reversible harm to the patient or user. No permanent damage or serious injury occurs.
- Marginal: Compromise of interface can cause a significant or total loss of product function, but does not represent an immediate risk of injury. No permanent damage or serious injury occurs.
- Negligible: Compromise of interface cannot cause injury and causes at most a minor loss of product function. Surgery can be completed with da Vinci system.

There are six Likelihood rankings defined in DOP 854136. With respect to cybersecurity risks, these rankings are interpreted as follows:

- Frequent: Compromise of interface can cause injury and interface is trivially compromised, e.g. utilizes an industry-standard networked communications protocol with no security mitigations.

- Probable: Compromise of interface can cause injury and interface is straightforward to compromise, e.g. utilizes a networkable interface with few or no security mitigations.
- Occasional: Compromise of interface can cause injury and interface is not straightforward to compromise, e.g. utilizes a networkable interface with security mitigations, or a non-networkable interface that requires attacker to have direct physical connection to system.
- Remote: Compromise of interface can cause injury and interface is difficult to compromise, e.g. utilizes a networkable interface with layered security mitigations, or a non-networkable interface with security mitigations.
- Improbable: Compromise of interface is extremely unlikely to cause injury, or interface can cause injury but is extremely difficult to compromise, e.g. interface with several layers of mitigations or that requires design of custom tools for compromise
- Incredible: Interface compromise cannot cause injury by design.

The acceptability of each risk is evaluated on a three-region risk chart defined in DOP 854136 and presented below. The three regions of the chart describing the acceptability of each risk are:

- Intolerable Risks (I), highlighted in red.
- Undesirable Risks (II) and Tolerable Risks (III), highlighted in yellow.
- Broadly Acceptable Region (IV), highlighted in green.

Likelihood	Severity			
	Negligible	Marginal	Critical	Catastrophic
	Risk Index			
Frequent	II	I	I	I
Probable	III	II	I	I
Occasional	III	III	II	I
Remote	IV	III	III	II
Improbable	IV	IV	III	III
Incredible	IV	IV	IV	IV

The likelihood and severity associated with each risk are used to determine each risk's level of acceptability. That level of acceptability is then used to determine the level of mitigation required for each use scenario and hazard. Those risks classified with a Risk Index of I must be

mitigated to a lower risk index if possible. Those risks classified with a Risk Index of II or III should be mitigated further if practical. Those risks with a Risk Index of IV require no further mitigations.

Cybersecurity Risks

1 Common Interfaces (All Carts)

Sec.	ID(s)	Interface	Interface Function and Type	Detailed Hazard Identification	Consequence of Compromise	Severity	Mitigations	Post-Likelihood	Post-Risk Index
1.1	[redacted]								
1.2									

Risk Category Keys:

Risk Index
I : Intolerable Risk, II : Undesirable Risk
III : Tolerable Risk, IV : Broadly Acceptable

Sec.	ID(s)	Interface	Interface Function and Type	Detailed Hazard Identification	Consequence of Compromise	Severity	Mitigations	Post-Likelihood	Post-Risk Index
1.3	[redacted]								

2 Vision Cart Interfaces

Sec.	ID(s)	Interface	Interface Function and Type	Detailed Hazard Identification	Consequence of Compromise	Severity	Mitigations	Post-Likelihood	Post-Risk Index
2.1	[redacted]								
2.2									
2.3									

Risk Category Keys:

Risk Index
I : Intolerable Risk, II : Undesirable Risk
III : Tolerable Risk, IV : Broadly Acceptable

Sec.	ID(s)	Interface	Interface Function and Type	Detailed Hazard Identification	Consequence of Compromise	Severity	Mitigations	Post-Likelihood	Post-Risk Index
2.4	[redacted]								
2.5									
2.6									
2.7									

Risk Category Keys:

Risk Index
I : Intolerable Risk, II : Undesirable Risk
III : Tolerable Risk, IV : Broadly Acceptable

Sec.	ID(s)	Interface	Interface Function and Type	Detailed Hazard Identification	Consequence of Compromise	Severity	Mitigations	Post-Likelihood	Post-Risk Index
2.8	[redacted]								

3 Patient Cart Interfaces

Sec.	ID(s)	Interface	Interface Function and Type	Detailed Hazard Identification	Consequence of Compromise	Severity	Mitigations	Post-Likelihood	Post-Risk Index
3.1	164685	RFID reader on USM	Read / write data to instrument / scope RFID tag	Compromise of interface leads to modification of instrument / scope data or injection of false instrument / scope data.	Modification of instrument / scope parameters can cause incorrect motion control. Possible to use surgical instruments beyond tested life.	Critical	Communications between RFID reader and tag are encrypted.	Improbable	III
3.2	164687	RFID tag on instrument	Storage of instrument / scope data	Modification of instrument / scope data or injection of false instrument / scope data.	Modification of instrument / scope parameters can cause incorrect motion control. Possible to use surgical instruments beyond tested life.	Critical	Data on RFID tag are encrypted and password-protected. Encryption key and use counting data areas on RFID tag are one-time programmable and cannot be modified once written.	Improbable	III

Risk Category Keys:

Risk Index
I : Intolerable Risk, II : Undesirable Risk
III : Tolerable Risk, IV : Broadly Acceptable

CYLANCE

Professional Services

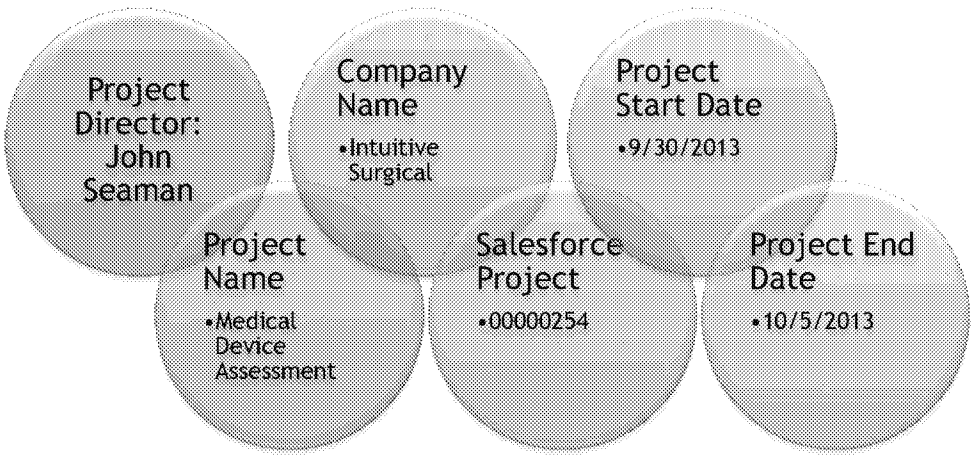
Technical Report

PREPARED NOVEMBER 15, 2013

CYLANCE, INC. | PROPRIETARY AND CONFIDENTIAL

Technical Report v1.0

DOCUMENT MANAGMENT



REVISION HISTORY:

EXECUTIVE SUMMARY

Table of Contents:

VULNERABILITY SUMMARY & RECOMMENDATIONS

This test harness allows for test cases to be created programmatically on the assessment laptop, as opposed to test cases directly on the USB device itself. This allows for more efficient and rapid deployment of USB test cases against the daVinci. Each USB interface was subjected to [redacted]

No observable software faults or security issues were discovered during USB testing. USB test cases included:

- [redacted]

Specific test cases include:

- [redacted]

Despite numerous attempts against each interface, no significant issues were discovered. The specific testing harnesses for each of these test suites can be found in the Appendix to this report.

RFID TESTING

All RFID interfaces associated with the daVinci system were subjected to manual tests. Cylance created a custom RFID hardware testing harness to RFID exposures. The custom testing harness consisted of:

- [redacted]

[redacted]

VULNERABILITY SUMMARY & RECOMMENDATIONS

[redacted]

[redacted]

No observable software faults or security issues were discovered during RFID testing. RFID test cases included:

- [redacted]

DVI TESTING

All DVI interfaces associated with the daVinci system were subjected to manual and automated tests. Cylance created a custom DVI hardware testing harness to DVI exposures. The custom testing harness consisted of:

- [redacted]

Unlike other testing harnesses, [redacted] No observable software faults or security issues were discovered during DVI interface testing. DVI test cases included:

- [redacted]

INTUITIVE SURGICAL

Validation Protocol, IS4000, Cybersecurity & Penetration Testing

DOCUMENT: 818460-40P
REVISION: A

Title

818460-40P Revision A, Validation Protocol, IS4000, Cybersecurity & Penetration Testing

Table of Contents

INTUITIVE SURGICAL

Validation Protocol, IS4000, Cybersecurity & Penetration Testing

DOCUMENT: 818460-40P
REVISION: A

Originator

Zachary Dickinson

Protocol Approval

Required approvals are defined in 853029 DOP, Signature Matrix.

See ECO C98466 for electronic approval signatures.

Purpose

This protocol describes the procedures for Cybersecurity and penetration testing of the test article defined below. The purpose of this testing is to confirm that the test article meets the specifications listed below.

Requirement(s) or Specification(s) being Verified or Validated by this protocol	814043 Rev. N Product Requirements, IS4000 (Cybersecurity Requirements)
Test Article Name(s)	IS4000 Surgical System SOFTWARE, IS4000, A70_P2 Release

INTUITIVE SURGICAL

Validation Protocol, IS4000, Cybersecurity & Penetration Testing

DOCUMENT: 818460-40P
REVISION: A

Equipment, Fixture, Tool	PMC Asset No.	PM Next Due	Tester Initials / Date
See reports attached	N/A	N/A	ZJD 2/3/14
N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A

Validation Protocol, IS4000, Cybersecurity & Penetration Testing

DOCUMENT: 818460-40P, **REVISION:** A

Test Protocol ← | → Test Results

Sec.	ID(s)	Test Case Name	Test Case Setup Instructions	Acceptance Criteria	Observed Results (Recorded During Test Execution)	Pass/ Fail Initials & Date	Notes
			and perform penetration attacks on each I2C port to inject system commands	observed.	as expected	N/A	N/A
7	1032813	RFID Reader	1. Place IS4000 in following mode and periodically perform simulated surgical tasks with periodic instrument changes. 2. Scan and probe each RFID reader. 3. Attempt to establish a communications path and perform penetration attacks on each RFID reader.	2. No unintended system movement or non-intuitive motion of the system is observed. 3. No unintended system movement or non-intuitive motion of the system is observed.	as expected	(P) / F ZJD 10/4/13	N/A
8	1032798	Serial Ports	1. Place IS4000 in following mode and periodically perform simulated surgical tasks. 2. Scan and probe each external serial port. 3. Attempt to establish a communications path and perform penetration attacks on each Serial port to inject system commands	2. No unintended system movement or non-intuitive motion of the system is observed. 3. No unintended system movement or non-intuitive motion of the system is observed.	as expected	(P) / F ZJD 10/4/13	N/A
9	1032796	Ethernet Ports	1. Place IS4000 in following mode and periodically perform simulated surgical tasks.	2. No unintended system movement or non-intuitive motion of the system is	as expected	(P) / F ZJD 10/4/13	N/A

Validation Protocol, IS4000, Cybersecurity & Penetration Testing

DOCUMENT: 818460-40P, **REVISION:** A

Test Protocol ← | → Test Results

Sec.	ID(s)	Test Case Name	Test Case Setup Instructions	Acceptance Criteria	Observed Results (Recorded During Test Execution)	Pass/ Fail Initials & Date	Notes
			2. Scan and probe each external Ethernet port. 3. Attempt to establish a communications path and perform penetration attacks on each Ethernet port to inject system commands	observed. 3. No unintended system movement or non-intuitive motion of the system is observed.	as expected	N/A	N/A
10	1032890	RFID Tag	1. Scan and probe each RFID instrument and Endoscope tag. 2. Attempt to establish a communications path and read, write or modify RFID tag data. 3. Insert instrument and Endoscope in IS4000 system and perform simulated surgical task.	2. Data on the tag cannot be read, written or modified. 3. No unintended system movement or non-intuitive motion of the system is observed.	as expected	(P) / F ZD 10/4/13	N/A